

# **Method, System, and Data Structure for Trustworthy Digital Document Interchange and Preservation**

## **CLAIMS OF THIS INVENTION**

- 555 1) A method for packaging information objects wherein the package includes an identifier of the package object itself and the whole is sealed by cryptographic message authentication
- 2) The method of claim (1), wherein the private key portion of a public/private key pair used for sealing is protected by use only in subsystems disconnected from networks and, optionally, is frequently replaced.
- 560 3) The method of claim (1), wherein a public key associated with the claim (2) private key is published and optionally endorsed by a certificate signed by an institution other than that to which the keys alluded to in claim (2) belong, with this endorsing institution having a business dependency on its reputation for care, know-how, and integrity.
- 4) The method of claim (1), including within the package a record describing a link between two information objects by referencing their identifiers or indices.
- 565 5) The method of claim (1), including within the package metadata recording a value that binds an external object defining a well-known ontology to an included payload element or link.
- 6) The method of claim (1), wherein an information object X included in the new package Z is itself packaged as described in claim (1) and wherein the identifier of Z alluded to in claim (1) has the same value as the identifier of X.
- 570 7) A method for packaging an information object with metadata not otherwise provided, where such metadata includes software or instructions for interpretation of the information object, or alternatively contains a reference to a durable external deposit of such software or instructions.

- 8) The method of claim (7), wherein the information object and the information enabling its interpretation are bound together by a cryptographic message authentication code.
- 575 9) The method of claim (7), wherein the software for interpretation is encoded with the instruction set of a machine, called a Universal Virtual Computer (**UVC**), that is simple enough for complete specification so that it can be emulated without error or omission by any sufficiently skilled third party who has the specification of this **UVC**.
- 580 10) The method of claim (7), wherein the software and instructions alluded to implement well-known methods that are made reliably interpretable by their schema being standardized and identified by or included in the package.
- 11) A system for packaging information objects wherein the package created includes an identifier of the package object itself and the package is sealed by cryptographic message authentication.
- 585 12) The system of claim (11), wherein the private key portion of a public/private key pair used for sealing is protected by use only in subsystems disconnected from networks and, optionally, is frequently replaced.
- 13) The system of claim (11), wherein a public key associated with the claim (12) private key is published and optionally endorsed by a certificate signed by an institution other than that to which the keys alluded to in claim (12) belong, with this endorsing institution having a business dependency on its reputation for care, know-how, and integrity.
- 590 14) The system of claim (11), including within the package created a record describing a link between two information objects by referencing their identifiers or indices.
- 15) The system of claim (11), including within the package metadata recording a value that binds an external object defining a well-known ontology to an included payload element or link.
- 595 16) The system of claim (11), wherein an information object X included in the new package Z is itself packaged as described in claim (11) and wherein the identifier of Z alluded to in claim (11) has the same value as the identifier of X.

- 17) A system for packaging an information object together with metadata not otherwise provided, where  
600 such metadata includes software or instructions for interpretation of the information object, or  
alternatively contains a reference to a durable external deposit of such software or instructions.
- 18) The system of claim (17), wherein the information object and the information enabling its  
interpretation are bound together by a cryptographic message authentication code.
- 19) The system of claim (17), wherein the software for interpretation is encoded with the instruction set  
605 of a machine, called a Universal Virtual Computer (**UVC**), that is simple enough so that it can be  
emulated without error or omission by any sufficiently skilled third party who has the specification of  
this **UVC**.
- 20) The system of claim (17), wherein the software and instructions alluded to implement well-known  
methods that are made reliably interpretable by their schema being standardized and either identified  
610 or included in the package.
- 21) An article of manufacture containing packaged information objects wherein the package includes an  
identifier of the package object itself and the package is sealed by cryptographic message  
authentication.
- 22) The article of manufacture of claim (21), wherein the private key portion of a public/private key pair  
used for sealing is protected against misappropriation by use only in subsystems disconnected from  
615 networks and, optionally, is frequently replaced.
- 23) The article of manufacture of claim (21), wherein a public key associated with the claim (22) private  
key is published and optionally endorsed by a certificate signed by an institution other than that to  
which the keys alluded to in claim (22) belong, with this endorsing institution having a business  
620 dependency on its reputation for care, know-how, and integrity.
- 24) The article of manufacture of claim (21), including the package recording a link between two  
information objects by referencing their identifiers or indices.
- 25) The article of manufacture of claim (21), including within the package metadata recording a value  
that binds an external object defining a well-known ontology to an included payload element or link.

- 625 26) The article of manufacture of claim (21), wherein an information object X included in the package Z is itself packaged as described in claim (21) and wherein the identifier of Z alluded to in claim (21) has the same value as the identifier of X.
- 27) An article of manufacture that packages an information object together with metadata not otherwise provided, where such metadata includes software or instructions for interpretation of the information object, or alternatively contains a reference to a durable deposit of such software or instructions.
- 630 28) The article of manufacture of claim (27), wherein the information object and the information enabling its interpretation are bound together by a cryptographic message authentication code.
- 29) The article of manufacture of claim (27), wherein the software for interpretation is encoded with the instruction set of a machine, called a Universal Virtual Computer (**UVC**), that is simple enough so that it can be emulated without error or omission by any sufficiently skilled third party who has the specification of this **UVC**.
- 635 30) The article of manufacture of claim (27), wherein the software and instructions alluded to implement well-known methods that are made interpretable by their schema being standardized and identified or included in the package.

640  
635  
630  
625  
620  
615  
610  
605  
600  
595  
590  
585  
580  
575  
570  
565  
560  
555  
550  
545  
540  
535  
530  
525  
520  
515  
510  
505  
500  
495  
490  
485  
480  
475  
470  
465  
460  
455  
450  
445  
440  
435  
430  
425  
420  
415  
410  
405  
400  
395  
390  
385  
380  
375  
370  
365  
360  
355  
350  
345  
340  
335  
330  
325  
320  
315  
310  
305  
300  
295  
290  
285  
280  
275  
270  
265  
260  
255  
250  
245  
240  
235  
230  
225  
220  
215  
210  
205  
200  
195  
190  
185  
180  
175  
170  
165  
160  
155  
150  
145  
140  
135  
130  
125  
120  
115  
110  
105  
100  
95  
90  
85  
80  
75  
70  
65  
60  
55  
50  
45  
40  
35  
30  
25  
20  
15  
10  
5  
4  
3  
2  
1  
0